APROVADO PELA RESOLUÇÃO CA BNDES Nº 03/2025

FOLHA DE INFORMAÇÕES GERAIS DO ATO NORMATIVO

Título
POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO DO SISTEMA BNDES (PCSI)

Unidade Gestora	**Unidade(s) Corresponsável(is)**
DEPARTAMENTO DE GESTÃO DE RISCO OPERACIONAL DA ÁREA DE INTEGRIDADE E COMPLIANCE (AIC/DEROP)	

Tipo de normativo				
☒ Política	☐ Regulamento	☐ Ato Organizacional	☐ Procedimento	☐ Circular

Previsão de delegação de competência		
☒ Não há	☐ Diretoria para Diretor / Presidente ☐ Diretoria para Comitês ☐ Diretoria para Superintendente	
☐ CA para Diretoria		
☐ Diretor para Superintendente	☐ Outro (especificar)	

Legislação de Referência

DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018 (INSTITUI A POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO E DISPÕE SOBRE A GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL)

DECRETO Nº 10.222, DE 05 DE FEVEREIRO DE 2020 (QUE INSTITUI A ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA)

INSTRUÇÃO NORMATIVA Nº 1, DE 27 DE MAIO DE 2020 (DISPÕE SOBRE A ESTRUTURA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO NOS ÓRGÃOS E NAS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL)

INSTRUÇÃO NORMATIVA GSI/PR Nº 3, DE 28 DE MAIO DE 2021 (DISPÕE SOBRE OS PROCESSOS RELACIONADOS À GESTÃO DE SEGURANÇA DA INFORMAÇÃO NOS ÓRGÃOS E NAS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL, ESPECIALMENTE MAPEAMENTO DE ATIVOS DE INFORMAÇÃO E GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO)

INSTRUÇÃO NORMATIVA GSI/PR Nº 5, DE 30 DE AGOSTO DE 2021 QUE DISPÕE SOBRE OS REQUISITOS MÍNIMOS DE SEGURANÇA DA INFORMAÇÃO PARA UTILIZAÇÃO DE SOLUÇÕES DE COMPUTAÇÃO EM NUVEM PELOS ÓRGÃOS E PELAS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL.

INSTRUÇÃO NORMATIVA GSI/PR Nº 6 DE 23 DE DEZEMBRO DE 2021 QUE ESTABELECE DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO PARA O USO SEGURO DE MÍDIAS SOCIAIS NOS ÓRGÃOS E NAS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL.

RESOLUÇÃO CMN Nº 4.893, DE 26 DE FEVEREIRO DE 2021 (DISPÕE SOBRE A POLÍTICA DE SEGURANÇA CIBERNÉTICA E SOBRE OS REQUISITOS PARA A CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM A SEREM OBSERVADOS PELAS INSTITUIÇÕES AUTORIZADAS A FUNCIONAR PELO BANCO CENTRAL DO BRASIL)

Atos Internos Relacionados

POLÍTICA CORPORATIVA DE PROTEÇÃO DE DADOS PESSOAIS DO SISTEMA BNDES (RESOLUÇÃO CA BNDES Nº 14/2021, DE 11/08/2021)

APROVADO PELA RESOLUÇÃO CA BNDES Nº 03/2025

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI – RESOLUÇÃO CA BNDES Nº 23/2023, DE 15/12/2023, E ALTERAÇÕES)

Processos Associados

GESTÃO DE RISCOS, CONTROLES E COMPLIANCE - RCC GERIR SEGURANÇA DA INFORMAÇÃO

Parametrização em Sistema(s)

☒ Não há	☐ Habilitação	☐ Financiamento	☐ Acompanhamento

Vigência		**Prazo de Revisão**
Início	Data de publicação no Portal de Normas	Revisão anual a contar da entrada em vigor.
Fim	N/A	

Palavras-chave (indexação)

SEGURANÇA DA INFORMAÇÃO, RISCOS CIBERNÉTICOS, CIBERSEGURANÇA. PCSI.

Atendimento de dúvidas

GSEG@BNDES.GOV.BR

APROVADO PELA RESOLUÇÃO CA BNDES nº 03/2025

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO DO SISTEMA BNDES (PCSI)

1. OBJETIVO

1.1. Esta Política estabelece os princípios, as diretrizes, os papéis e as responsabilidades que devem ser observados por todos os colaboradores na execução de processos das Empresas do Sistema BNDES para preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações produzidas ou recebidas e sob a custódia do BNDES.

2. ABRANGÊNCIA E ESCOPO

2.1 Esta Política é aplicável às atividades do BNDES e de suas subsidiárias, a BNDES Participações S/A (BNDESPAR) e a Agência Especial de Financiamento Industrial S.A. (FINAME).

2.1.1 Esta Política se aplica a todos os Participantes do Sistema BNDES e aos seus prestadores de serviço.

2.1.2 O escopo da aplicabilidade de normas complementares ou de diretrizes dessa PCSI em contratos de prestação de serviços pode, por interesse das Empresas do Sistema BNDES e do prestador, ser delimitado para excetuar itens não aplicáveis no âmbito do serviço prestado mediante a reavaliação do risco de segurança da informação e da anuência da unidade gestora de segurança da informação.

2.2 Esta Política, alinhada à missão e aos objetivos da Instituição, estabelece objetivos, princípios e responsabilidades aplicáveis aos processos de gestão de segurança da informação.

2.3 A gestão de segurança da informação do Sistema BNDES orienta-se essencialmente pelo disposto na Resolução CMN nº 4.893, de 26/02/2021, pelo Decreto 9.637, de 26/12/2018 e pelas Instruções Normativas GSI-PR nº 01, de 27/05/2020, nº 03 de 28/05/2021 e nº 05 de 30/08/2021.

2.4 Toda informação produzida, recebida, adquirida ou custodiada pelas Empresas do Sistema BNDES é considerada patrimônio das Empresas do Sistema BNDES e deve ser usada exclusivamente para atender a interesses institucionais.

APROVADO PELA RESOLUÇÃO CA BNDES nº 03/2025

3. DEFINIÇÕES E ABREVIATURAS

a) **Autenticidade:** propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado equipamento, sistema, órgão ou entidade.

b) **Confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, sistema, órgão ou à entidade não autorizados nem credenciados.

c) **Colaboradores:** todos os Participantes do Sistema BNDES, o que inclui os empregados e estagiários do BNDES, bem como prestadores de serviço e aprendizes**.**

d) **Informações sensíveis:** são aquelas classificadas como confidenciais, reservadas ou secretas de acordo com o normativo interno que dispõe sobre a classificação e tratamento de informações.

e) **Disponibilidade:** propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade.

f) **Integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

g) **Participantes do Sistema BNDES**: empregados integrantes dos quadros de pessoal permanente ou temporário, ainda que se encontrem cedidos ou requisitados ou liberados no âmbito do Acordo Coletivo de Trabalho do Sistema BNDES ou legislação específica, ou em gozo de licença ou em outro afastamento equivalente, com ou sem remuneração, os cedidos às empresas do Sistema BNDES, os estagiários e os membros dos órgãos colegiados estatutários das empresas do Sistema BNDES.

h) **Risco à Segurança da Informação:** potencial de violação da integridade, confidencialidade, disponibilidade ou autenticidade da informação de propriedade ou custodiada pelo Sistema BNDES em decorrência da exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo às Empresas do Sistema BNDES. Esta definição inclui o risco cibernético, que é o risco à segurança da informação que envolve ativo de tecnologia da informação.

i) **Serviços de tecnologia da informação relevantes**: são aqueles que manipulam informações sensíveis ou que suportam os sistemas principais de tecnologia da informação imprescindíveis para continuidade de processos críticos de negócio.

j) **Sistemas principais**: são aqueles referenciados no Plano Estratégico de Tecnologia da Informação[1]**.**

3.1 Para fins desta PCSI e seus anexos, consideram-se ainda as definições descritas no Manual de Conceitos, documento que é apresentado como o Anexo I desta Política e que é suficiente para o entendimento dos termos das demais Normas Complementares.

4. PRINCÍPIOS E DIRETRIZES

4.1 Os colaboradores devem observar os seguintes **princípios** de Segurança da Informação em suas decisões e na condução de suas atividades:

a) **privilégio mínimo:** os colaboradores devem possuir apenas os privilégios estritamente necessários ao desempenho das suas atribuições profissionais;

b) **proteção em camadas:** o uso de controles complementares deve ser incentivado com vistas a aumentar a efetividade e a tolerância a falhas do conjunto;

c) **adoção de padrões abertos**: as implementações de soluções de segurança devem priorizar a adoção de padrões abertos, de acordo com as orientações do ePING (Padrões de Interoperabilidade do Governo Eletrônico);

d) **controle pautado pelo risco**: a implantação de controles deve ser iniciada pelos mais simples e priorizada de acordo com o resultado de análises de riscos de segurança da informação;

e) **custo-benefício**: os custos associados aos controles não devem ser superiores aos benefícios esperados em decorrência de sua implementação; e

f) **viabilidade**: a aplicabilidade de controles deve ser ponderada diante de sua efetividade e do eventual impacto ao cumprimento das necessidades de negócio;

4.2 Os colaboradores devem observar as seguintes **diretrizes fundamentais** de Segurança da Informação em suas decisões e na condução de suas atividades:

4.2.1 Os ativos de TI e os ativos de informação sob gestão do Sistema BNDES, o que não inclui dispositivos pessoais, devem ser utilizados para exercício de atividades profissionais voltadas aos interesses corporativos das Empresas

[1] De acordo com o PETI, são considerados sistemas principais de TI o portal institucional do BNDES (site do Banco na Internet) e aqueles cuja indisponibilidade causa impacto significativo nos processos fundamentais à atuação do Sistema BNDES, no mercado financeiro e de capitais, a saber: captação e gestão do passivo; realização de operações diretas, indiretas ou de renda variável; e cumprimento de obrigações ao Banco Central do Brasil (BACEN) e à Comissão de Valores Mobiliários (CVM).

do Sistema BNDES e em consonância com as atribuições de cada colaborador.

4.2.2 O acesso a informações sigilosas deve ser precedido da assinatura de um Termo de Confidencialidade baseado, conforme o caso, em um dos modelos anexos a essa Resolução e listados a seguir:

a) Modelo de Termo de Confidencialidade e Tratamento de Dados Pessoais para Contratos Administrativos (Anexo II);

b) Modelo de Termo de Confidencialidade e Tratamento de Dados Pessoais para Profissionais e Estagiários das Empresas do Sistema BNDES (Anexo III);

c) Modelo de Termo de Confidencialidade e Tratamento de Dados Pessoais para Profissionais Terceirizados (Anexo IV);

d) Modelo de Termo de Confidencialidade e Tratamento de Dados Pessoais para Empresas na Ausência de Contrato (Anexo V); e

e) Modelo de Termo de Confidencialidade e Tratamento de Dados Pessoais para Pessoa Física na Ausência de Contrato (Anexo VI).

4.2.3 Os colaboradores devem comunicar imediatamente a unidade gestora de Segurança da Informação sempre que tomarem conhecimento de vulnerabilidades, indícios de comprometimento de ativos de informação e casos de desrespeito à PCSI.

4.2.4 Todos os incidentes de Segurança da Informação, comunicados às Empresas do Sistema BNDES ou verificados por seus próprios colaboradores, devem ser analisados, classificados de acordo com sua relevância, contidos e tratados.

4.2.5 Os colaboradores que identificarem vulnerabilidades em ativos de TI não devem tentar testá-las ou explorá-las sem autorização da unidade gestora de Segurança da Informação.

4.2.6 As configurações dos ativos de TI não devem ser alteradas com a finalidade de burlar os controles aplicados ou de permitir acessos não autorizados.

4.3 A UF Gestora de Tecnologia da Informação deve observar as seguintes **diretrizes fundamentais** de Segurança da Informação em suas decisões e na condução de suas atividades:

4.3.1 A introdução de ativos de Tecnologia da Informação para execução em regime de produção, bem como a implementação de mudanças nesses ativos devem ser precedidas de homologação que inclua avaliação do impacto à segurança e verificação de conformidade com as diretrizes, normas e padrões internos.

APROVADO PELA RESOLUÇÃO CA BNDES nº 03/2025

4.3.2 Os ativos de Tecnologia da Informação utilizados pelas Empresas do Sistema BNDES devem ser inventariados, protegidos, possuir responsável definido para sua gestão e ter o acesso controlado para assegurar que somente pessoas autorizadas possam deles se utilizar, em conformidade com o princípio do privilégio mínimo.

4.3.3 O processo de desenvolvimento de sistemas deve ser realizado em conformidade com as diretrizes, normas e padrões definidos internamente para este fim, bem como estar de acordo com as melhores práticas de Segurança da Informação.

4.3.4 O projeto de sistemas desenvolvidos ou adquiridos deve:

a) contemplar as funcionalidades relacionadas ao controle de acesso à informação e à comunicação de dados, em conformidade com as diretrizes, normas e padrões internos;

b) ser precedido de uma avaliação acerca do tratamento de informações sensíveis, que considere especialmente aos requisitos para proteção dos dados pessoais, inclusive a garantia ao direito de privacidade;

c) considerar a implementação dos controles necessários para tratar adequadamente riscos de segurança da informação e a titulares de dados pessoais, que tenham sido previamente mapeados, para os casos de uso em desenvolvimento; e

d) priorizar o uso das bases corporativas de credenciais e privilégios de acessos.

4.3.5 Os privilégios de acesso atribuídos aos colaboradores devem ser construídos de acordo com os papéis de negócio e atributos organizacionais reconhecidos pelas Empresas do Sistema BNDES.

4.4 As Unidades Administrativas e os colaboradores devem observar as seguintes **diretrizes fundamentais** ao classificar ou tratar informações das Empresas do Sistema BNDES:

4.4.1 A classificação de informações deve observar a publicidade como preceito geral e a atribuição do sigilo como exceção, conforme inciso I do artigo 3º da Lei 12.527, de 18/11/2011 (Lei de Acesso à Informação), e o princípio da transparência, conforme item 4 da Política de Transparência do Sistema BNDES, aprovada pela Resolução DIR BNDES nº 2.880, de 18/09/2015 e suas alterações.

4.4.2 As informações devem ser classificadas e tratadas segundo critérios e procedimentos estabelecidos em normativo próprio, atualmente a OS PRESI BNDES nº 01, de 22/01/2015, e suas eventuais alterações posteriores.

4.4.3 Na ausência de justificativas legais para a atribuição de restrição de acesso à informação, o seu gestor deve utilizar os instrumentos previstos no ato

normativo referenciado no item 4.4.2 para tornar evidente o caráter público da informação.

4.4.4 Os colaboradores devem observar as orientações no ato normativo referenciado no item 4.4.2 para garantir o adequado tratamento às informações sigilosas, especialmente para evitar sua exposição indevida, o que começa com a adoção de cuidados básicos como, por exemplo, a guarda dos documentos em gavetas ou arquivos com tranca, a manutenção da mesa sem documentos ou informações sigilosas (mesa limpa) e a estação de trabalho bloqueada nos momentos de ausência de uso.

4.4.5 Os ativos de informação utilizados pelas Empresas do Sistema BNDES devem ser protegidos, possuir responsável definido para sua gestão e ter o acesso controlado para assegurar que somente pessoas autorizadas possam deles se utilizar, em conformidade com o princípio do privilégio mínimo.

4.4.6 O tratamento de informação relacionada à pessoa natural identificada ou identificável, especialmente de dados pessoais sensíveis, deve observar as diretrizes e regras estabelecidas na Política Corporativa de Proteção de Dados Pessoais do Sistema BNDES (PCPD), com destaque à necessidade de o tratamento de dados pessoais realizar-se com base em uma das situações admitidas na legislação; e do cumprimento dos princípios da finalidade, da adequação, da necessidade, da transparência, da segurança e da prevenção.

4.4.7 A disponibilidade e a proteção das informações devem ocorrer de acordo com a sua classificação e de forma a preservar a continuidade de negócios das Empresas do Sistema BNDES.

4.4.8 Cláusulas de sigilo e confidencialidade devem constar nos contratos estabelecidos com profissionais terceirizados, prestadores de serviços e estagiários.

4.5 Devem ser observadas as diretrizes corporativas para controles internos, gestão de riscos e continuidade do negócio, de forma a preservar os ativos de informação necessários à sustentação das operações das Empresas do Sistema BNDES.

4.6 A elaboração de cenários de incidentes considerados nos testes de continuidade de negócio deve contemplar riscos cibernéticos que possam afetar a disponibilidade dos processos críticos de negócio.

4.7 Periodicamente devem ser realizados treinamentos que incluam aspectos de segurança da informação ou avaliações sobre a prontidão dos colaboradores em identificar e em notificar tempestivamente a unidade gestora de segurança da informação sobre ameaças cibernéticas.

APROVADO PELA RESOLUÇÃO CA BNDES nº 03/2025

5. PAPÉIS E RESPONSABILIDADES

5.1 Cabe ao Conselho de Administração (CA):

a) deliberar para aprovação do Sistema de Gestão de Segurança da Informação (SGSI), da Política Corporativa de Segurança da Informação (PCSI), do Plano Estratégico de Segurança da Informação (PESI) e do Plano de Resposta a Incidentes de Segurança da Informação (PRISI), bem como atribuir as responsabilidades envolvidas, conforme estabelece o Decreto 9.637 de dezembro de 2018 e a Resolução CMN nº 4.893 de 2021 ou outros normativos que os substituam.

b) apoiar e promover as iniciativas para fortalecimento da segurança da informação.

c) acompanhar a execução dos planos e de indicadores que compõem o SGSI.

5.2 Cabe ao Comitê de Riscos (CR):

a) propor, com periodicidade mínima anual, recomendações ao Conselho de Administração sobre esta política e sobre os planos para gestão de segurança da informação que compõem o SGSI;

b) analisar o ambiente de riscos de segurança da informação do Sistema BNDES, mediante informações produzidas pela AIC;

c) supervisionar a atuação e desempenho do Diretor Responsável por Segurança da Informação;

d) avaliar o grau de aderência dos processos da estrutura de gerenciamento de riscos às políticas estabelecidas;

e) apoiar o Conselho de Administração com a avaliação dos planos de ação e tratamento de incidentes de segurança da informação, da política de segurança da informação e das demais normas que tratam do tema no âmbito interno; e

f) apreciar o relatório anual sobre a implantação dos planos de ação e de tratamento de incidentes de segurança da informação, relatório que atualmente compõe o RARO (Relatório Anual de Gestão de Risco Operacional, Controle Interno e Compliance).

5.3 Cabe à Diretoria Executiva:

a) manifestar-se acerca de propostas para aprovação das políticas, planos e normas que compõem o SGSI e sobre o próprio SGSI, submetendo-os para deliberação do Conselho de Administração;

b) apoiar e promover as iniciativas para fortalecimento da segurança da informação; e

c) promover a execução das ações para segurança da informação previstas no PESI.

APROVADO PELA RESOLUÇÃO CA BNDES nº 03/2025

5.4 Cabe ao Diretor Responsável por Segurança da Informação:

a) zelar pelo cumprimento desta PCSI;

b) deliberar sobre a criação, alteração ou eliminação de normas complementares a essa PCSI e de seus demais anexos;

c) acompanhar periodicamente os indicadores e os planos do SGSI;

d) orientar sobre a definição de prioridades nas ações previstas no PESI, bem como zelar por sua adequada execução.

e) garantir os recursos necessários para implantação e acompanhamento dos controles previstos nesta PCSI; e

f) atuar como responsável do Sistema BNDES junto ao Banco Central do Brasil nos assuntos afetos à Segurança da Informação, nos limites da Resolução CMN nº 4.893, de 26/02/2021 ou outro normativo que o substitua.

5.5 Cabe ao Comitê de Segurança da Informação (CSI):

a) propor ou avaliar alterações nas políticas, planos e normas que compõem o SGSI e encaminhá-la para deliberação da Diretoria Executiva;

b) deliberar sobre o tratamento de casos excepcionais encaminhados para apreciação do comitê;

c) assessorar na implementação das ações de segurança da informação;

d) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação;

e) acompanhar os indicadores e a execução dos planos que compõem o SGSI;

f) promover a governança de Segurança da Informação e o adequado alinhamento estratégico das ações de segurança da informação; e

g) apreciar os relatórios sobre a utilização de mídias sociais e os relacionados aos incidentes de segurança ocorridos em perfis institucionais em mídias sociais.

5.6 Cabe ao Comitê de Gestão de Riscos (CGR):

a) avaliar o processo de gestão dos riscos de segurança da informação;

b) apoiar a gestão de riscos de segurança da informação de forma integrada aos demais riscos, fomentando o desenvolvimento de metodologias para uma visão unificada de riscos e que possibilitem a identificação, a mensuração, a avaliação, o monitoramento, o reporte, o controle e a mitigação dos efeitos resultantes das interações dos riscos de segurança da informação com os demais riscos; e

c) analisar os trabalhos relativos à gestão de riscos de Segurança da Informação, com vistas a ratificar, alterar ou recomendar ações de tratamento e/ou aprimoramento dos controles e procedimentos, e acompanhar sua implementação pelas UFs envolvidas.

5.7 Cabe à Unidade Fundamental Gestora de Tecnologia de Informação:

a) avaliar os potenciais impactos à segurança da informação que possam ocorrer na implementação de mudanças de TI, bem como verificar o resultado dessas mudanças e propor controles para mitigar os riscos de SI gerados por elas;

b) adotar as melhores práticas para segurança na implantação e no desenvolvimento de sistemas sob sua responsabilidade;

c) manter e acompanhar o inventário de Ativos de Informação em meio eletrônico e de Ativos de TI com o objetivo de manter atualizado um banco de dados de gerenciamento de configuração e promover a adequada identificação e classificação dos ativos; e

d) apoiar o Gestor de Licença de *Software* na realização do inventário da utilização de licenças e apoiar na geração de evidências para auditorias de licença de *software*.

5.8 Cabe à Unidade de Integridade e Compliance (AIC):

a) elaborar, manter e revisar periodicamente os documentos que compõem o SGSI, o que inclui a PCSI, o PRISI e o PESI, à luz das orientações do Gestor de Segurança da Informação, bem como zelar pela observância das políticas e a execução das ações de Segurança da Informação;

b) definir, medir e apresentar os indicadores selecionados do SGSI e os principais resultados das ações planejadas no PESI aos colegiados e integrantes da estrutura de gestão e governança de SI;

c) garantir a adequada resposta e tratamento de incidentes de Segurança da Informação, de acordo com o PRISI e a execução dos serviços de segurança previstos;

d) secretariar o Comitê de Segurança da Informação;

e) acompanhar os indicadores dos processos e dos planos que compõem o SGSI e apresentá-los periodicamente ao Gestor de Segurança da Informação e, quando demandado, aos demais colegiados que compõe a estrutura de gestão de Segurança da Informação;

f) apoiar o acionamento do Plano de Gerenciamento de Incidentes do Sistema BNDES (PGI) sempre que um incidente de segurança impacte em um incidente, contingência ou crise no escopo da continuidade de negócios, conforme define a Política Corporativa de Gestão de Continuidade de Negócios (atualmente a Resolução CA BNDES nº 15/2024);

g) elaborar os planos e os relatórios para gestão de riscos de segurança da informação;

h) elaborar o relatório de incidentes de segurança ocorridos em perfis institucionais em mídias sociais e encaminhá-lo ao Gestor de Segurança da Informação;

i) coordenar a equipe de tratamento de incidentes de segurança da informação em rede do Sistema BNDES;

j) definir e adotar procedimentos para o adequado tratamento de incidentes de segurança da informação em rede do Sistema BNDES;

k) atuar como ponto focal para comunicação com entidades externas, ressalvada a atribuição do Encarregado de Proteção de Dados Pessoais do Sistema BNDES, nos termos definidos na PCPD, e com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV, nos assuntos relativos a incidentes de segurança da informação em rede do Sistema BNDES;

l) coordenar, quando demandado, as investigações, as avaliações dos danos decorrentes de quebras de segurança da informação e zelar pela adequada coleta de evidências;

m) disseminar a cultura de segurança da informação, com a implementação de programas de capacitação e de avaliação periódica de pessoal e apoiar as demais unidades na prestação de informações a clientes sobre riscos cibernéticos na utilização de produtos e serviços, inclusive na comunicação institucional por meio de mídias sociais;

n) acompanhar o processo de gestão de acessos a ativos de tecnologia da informação;

o) realizar estudos sobre novas tecnologias e seu potencial impacto à Segurança da Informação;

p) divulgar amplamente a PCSI a todos os colaboradores do Sistema BNDES, disponibilizar seu conteúdo integralmente para consulta interna e divulgar um resumo com as linhas gerais da norma ao público externo;

q) integrar o Comitê de Mudanças de Tecnologia da Informação, nos termos do normativo que regulamenta a atuação do Comitê (atualmente a Res DIR nº 3.944/2022-BNDES);

r) coordenar a execução do mapeamento de ativos de informações sensíveis e zelar por sua atualização periódica;

s) definir a metodologia para a execução do mapeamento de informações sensíveis, bem como consolidar as informações resultantes;

t) apoiar a avaliação dos riscos de segurança da informação e a elaboração dos planos de ação para tratamento de riscos cibernéticos, bem como promover seu adequado acompanhamento;

u) gerenciar, acompanhar e analisar, de forma contínua, as práticas de uso institucional seguro de mídias sociais, com relação aos aspectos de segurança da informação;

5.9 Cabe aos gestores de sistemas e de processos:

a) definir os requisitos de segurança da informação dos sistemas e processos sob sua responsabilidade e buscar assegurar-se de que tais exigências sejam cumpridas;

b) priorizar a correção de problemas e vulnerabilidades de segurança descobertas nos sistemas e processos sob sua responsabilidade;

c) aprovar os privilégios dos colaboradores que utilizam os sistemas ou atuam nos processos sob sua responsabilidade, bem como revisar periodicamente esses privilégios com vistas a revogar aqueles que não são mais necessários;

d) aprovar as declarações de aplicabilidade e o plano de tratamento de riscos de sistemas ou processos sob sua responsabilidade e acompanhar a execução do plano de tratamento de riscos;

e) fornecer periodicamente para a unidade gestora de Segurança da Informação e para a UF Gestora de Tecnologia da Informação a lista de privilégios dos colaboradores que utilizam os sistemas ou atuam nos processos sob sua responsabilidade, quando o sistema em questão não for integrado com a base corporativa de credenciais e acessos;

f) fornecer à unidade gestora de Segurança da Informação informações referentes aos ativos com informações sensíveis envolvidos em processos sob sua gestão, seja na sua criação ou atualização e sempre que demandados; e

g) identificar e avaliar o risco de segurança da informação aos ativos de informação sensíveis tratados no âmbito do processo sob sua gestão;

5.10 Cabe às Unidades Fundamentais (UF) e seus executivos:

a) observar, na execução de suas atividades, as disposições desta Política;

b) reportar tempestivamente ao AIC/DEROP informações relativas aos riscos de segurança das informações dos seus processos de trabalho e às perdas deles oriundas, bem como sobre o andamento dos planos de ação ou outras iniciativas para a mitigação desses riscos, prioritariamente por meio de seus Agentes de Conformidade;

c) incentivar a participação dos colaboradores da UF nas ações de capacitação relacionadas à gestão de segurança da informação, bem como providenciar para que conheçam integralmente e atuem em conformidade com esta Política; e

d) revisar periodicamente os privilégios de acesso dos colaboradores sob sua responsabilidade, com vistas a revogar aqueles que não são mais necessários.

5.11 Cabe à Unidade Fundamental Responsável pela Comunicação Institucional:

a) criar, alterar, excluir e controlar os perfis institucionais em mídias sociais do órgão ou da entidade;

b) remover, tão logo tome conhecimento, postagens que atentem contra a segurança da informação;

c) elaborar relatório mensal sobre a utilização de mídias sociais sob sua administração e apresentar ao gestor de segurança da informação;

d) fornecer à unidade gestora de Segurança da Informação informações referentes aos eventos, no âmbito do uso e gestão de perfis institucionais em mídias sociais, que possam implicar em comprometimento da segurança das informações do Sistema BNDES.

5.12 Cabe aos gestores de informação: efetuar a classificação das informações das quais foi indicado como gestor, bem como avaliar os controles e procedimentos relativos às atividades ligadas ao ciclo de vida dessas informações.

5.13 Cabe aos gestores de licença de *software*:

a) estabelecer regras para a autorização e revogação do uso das licenças do *software*;

b) autorizar o uso das licenças do *software* para novos usuários, bem como eventuais remanejamentos das licenças;

c) autorizar o uso de recursos que alterem o quantitativo da licença de *software*, por exemplo, o aumento da capacidade de processamento;

d) controlar o quantitativo de licenças em uso;

e) inventariar periodicamente a utilização das licenças do *software*;

f) zelar para que o uso esteja em conformidade com a licença e os direitos de uso do *software*, bem como o respectivo contrato de aquisição do *software* quando aplicável; e

g) responder tempestivamente a auditorias internas e externas que se refiram à licença de *software*, bem como gerar as eventuais evidências solicitadas.

5.14 Cabe aos gestores de contrato:

a) providenciar para que os colaboradores terceirizados que atuem no âmbito de contratos sob sua gestão observem as orientações da PCSI aplicáveis;

b) providenciar a assinatura do termo de confidencialidade e acesso a dados pessoais pertinente por todos os colaboradores terceirizados que eventualmente atuem no âmbito de contratos sob sua gestão;

c) revisar periodicamente os privilégios de acesso dos colaboradores sob sua responsabilidade, com vistas a revogar aqueles que não são mais necessários; e

d) difundir e promover no âmbito de sua atuação e competência as boas práticas de segurança da informação definidas nesta PCSI e em suas normas complementares.

5.15 Cabe ao responsável pelo Processo Gerenciar Mudanças de Tecnologia da Informação estabelecido nos termos do Mapeamento dos Processos de TI do BNDES, aprovado pela IS SUP/ATI nº 03/2023 (e alterações):

a) coordenar a gestão de mudanças de Tecnologia da Informação;

b) garantir, no âmbito do processo de gestão de mudanças, a apreciação dos aspectos de segurança da informação;

c) garantir o alinhamento do processo de gestão de mudanças, no tocante aos aspectos de segurança da informação e aos resultados do processo de gestão de riscos; e

d) assegurar o registro de auditoria de todas as informações relevantes relacionadas com as mudanças.

5.16 Cabe especificamente ao Gestor de Segurança da Informação:

a) propor e encaminhar para deliberação as políticas, planos e normas que compõem o SGSI;

b) manter contato com o Departamento de Segurança da Informação e Comunicações (DSIC), do Gabinete de Segurança Institucional da Presidência da República (GSIPR), para o trato de assuntos relativos à Segurança da Informação;

c) remeter, quando demandado, os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação para o GSIPR;

d) promover a cultura de segurança da informação;

e) acompanhar, quando demandado, as investigações, as avaliações dos danos decorrentes de quebras de segurança e zelar pela adequada coleta de evidências;

f) realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação;

g) acompanhar a atuação da equipe de tratamento e resposta a incidentes de segurança da informação na rede do Sistema BNDES – ETIR-BNDES, bem como zelar por sua adequada coordenação;

h) promover a gestão de riscos de segurança da informação;

i) avaliar o plano para gestão de riscos de segurança da informação e dos relatórios para identificação, análise, avaliação e tratamento dos riscos de segurança da informação;

j) zelar pela adequada execução do processo de mapeamento de ativos de informação sensíveis e acompanhar seus indicadores;

k) zelar pela adequada avaliação dos aspectos de segurança da informação na execução do processo de mudanças de TI;

l) propor recursos necessários para as ações de Segurança da Informação em consonância com o Plano Estratégico de Segurança da Informação (PESI) das empresas do Sistema BNDES;

m) zelar pela atualização dos processos de Segurança da Informação e dos procedimentos de trabalho;

n) apresentar ao Comitê de Segurança da Informação os relatórios sobre a utilização de mídias sociais e de eventuais incidentes de segurança ocorridos em perfis institucionais em mídias sociais;

o) aprovar, acompanhar e dar publicidade aos indicadores do SGSI, bem como submeter os relatórios com dados relativos à gestão de Segurança da Informação para apreciação dos colegiados pertinentes que compõem a estrutura de gestão de Segurança da Informação; e

p) coordenar o Comitê de Segurança da Informação.

5.17 Cabe aos colaboradores:

a) zelar pela segurança das informações das Empresas do Sistema BNDES;

b) participar na realização de testes e treinamentos de segurança da informação, quando solicitado pelo AIC/DEROP; e

c) atuar em conformidade com esta PCSI.

5.18 Os papéis e responsabilidades atribuídos nesta seção não excluem os previstos em outros normativos internos ou externos.

6. MONITORAÇÃO

6.1 As Empresas do Sistema BNDES podem, a seu critério e, observadas as disposições da Lei nº 13.709, de 2018, bem como as regras estabelecidas pela PCPD, monitorar e registrar a manipulação de Ativos de Informação armazenados ou em trânsito, com o objetivo de zelar pelo fiel cumprimento da PCSI.

6.2 Os colaboradores usuários de Ativos de TI do Sistema BNDES devem ser informados da possibilidade de registro e monitoramento das atividades realizadas por meio desses ativos.

7. NORMAS COMPLEMENTARES

7.1 As normas apresentadas a seguir e apensadas a este documento complementam essa PCSI com diretrizes para procedimentos e controles específicos, além de regularem e atribuírem responsabilidades adicionais sobre os temas que endereçam, a saber:

7.1.1 Norma de Segurança da Informação para Acesso a Áreas com Ativos Críticos de Tecnologia da Informação (Anexo VII): estabelece que os ativos de Tecnologia da Informação considerados críticos ao desempenho das atividades das Empresas do Sistema BNDES devem ser armazenados em áreas apropriadas, com acesso restrito, e dispõe sobre:

a) autorização de acesso;
b) registro e monitoração de acesso; e
c) execução de procedimentos técnicos.

7.1.2 Norma de Segurança da Informação para Acesso Remoto a Ativos de Tecnologia da Informação (Anexo VIII): estabelece as responsabilidades e condições que devem ser observadas no acesso remoto a ativos de TI das Empresas do Sistema BNDES e dispõe sobre:

a) restrições para o uso;
b) solicitação e autorização;
c) controles necessários; e
d) auditoria do acesso.

7.1.3 Norma de Segurança da Informação para Controle de Acesso à Informação (Anexo IX): estabelece os requisitos para o controle de acesso à informação no âmbito das Empresas do Sistema BNDES e dispõe sobre:

a) credenciais de acesso;
b) senhas;
c) uso de dispositivos criptográficos;
d) autorização de acesso;
e) revisão e revogação de acessos;
f) auditoria; e
g) acesso a ativos de tecnologia da informação.

7.1.4 Norma para Gestão dos Serviços de Segurança da Informação (Anexo X): estabelece as diretrizes para a gestão dos processos de Segurança da Informação e dispõe sobre:

a) gestão de vulnerabilidades;
b) gestão de incidentes;
c) coleta de evidências e artefatos; e
d) intervenções em ativos de TI.

7.1.5 Norma de Segurança da Informação para Uso da Internet (Anexo XI): estabelece a conduta adequada para uso da Internet nas Empresas do Sistema BNDES e dispõe sobre:

a) uso aceitável da Internet;

b) controles empregados; e

c) monitoração dos acessos.

7.1.6 Norma de Segurança da Informação para Uso de Ativos de Tecnologia da Informação (Anexo XII): estabelece as responsabilidades e condições que devem ser observadas para uso de ativos de TI das Empresas do Sistema BNDES e dispõe sobre:

a) uso adequado dos ativos de TI;

b) uso dos ativos de TI por terceiros; e

c) uso das redes corporativas.

7.1.7 Norma de Segurança da Informação para Administração de Ativos de Tecnologia da Informação (Anexo XIII): estabelece as responsabilidades e condições que devem ser observadas para administração de ativos de TI das Empresas do Sistema BNDES e dispõe sobre:

a) administração de ativos de TI;

b) administração das redes corporativas;

c) inventário de ativos de TI; e

d) inventário de licenças de *software*.

7.1.8 Norma de Segurança da Informação para Uso do Correio Eletrônico (Anexo XIV): estabelece a conduta adequada dos colaboradores das Empresas do Sistema BNDES na utilização do correio eletrônico corporativo e dispõe sobre:

a) uso aceitável do serviço de correio eletrônico;

b) restrições quanto à comunicação externa;

c) arquivos anexos;

d) monitoração; e

e) conteúdo malicioso.

7.1.9 Norma de Segurança da Informação para Uso de Dispositivos Pessoais (Anexo XV): estabelece as responsabilidades e condições para uso de dispositivos pessoais conectados à infraestrutura de Tecnologia da Informação das Empresas do Sistema BNDES e dispõe sobre:

a) condição para uso de dispositivos pessoais na infraestrutura de TI do Sistema BNDES;

b) restrições quanto ao uso de dispositivos pessoais para acesso a recursos internos;

c) gerenciamento e controle;

d) monitoração; e

e) suporte.

7.1.10 Norma de Segurança da Informação para Uso de Serviços de Processamento, Armazenamento e Transmissão de Dados e Computação em Nuvem (Anexo XVI): estabelece os procedimentos e requisitos para uso de serviços de Tecnologia da Informação em nuvem para guarda, processamento ou transmissão de informações corporativas e dispõe sobre:

a) categorias de serviço de computação em nuvem;

b) restrições para o uso e análise preliminar de riscos;

c) autenticação, provisionamento e autorização;

d) auditoria e tratamento de incidentes de segurança;

e) controles exigidos;

f) continuidade do serviço; e

g) proteção dos dados e da comunicação.

7.1.11 Norma de Segurança da Informação para Uso Institucional de Mídias Sociais (Anexo XVII): estabelece a conduta adequada para uso e gestão de perfis institucionais das Empresas do Sistema BNDES mantidos em mídias sociais e dispõe sobre:

a) responsabilidades;

b) diretrizes e orientações para uso institucional seguro de mídias sociais; e

c) controles exigidos.

8. PENALIDADES

8.1 O descumprimento da PCSI pode acarretar responsabilização, nos termos dos respectivos regulamentos de pessoal dos Planos de Cargos e Salários das Empresas do Sistema BNDES e nos termos dos contratos ou convênios para

estagiários, menores aprendizes, empresas prestadoras de serviço e seus empregados, sem prejuízo das responsabilidades civis e penais eventualmente cabíveis.

9. DISPOSIÇÕES FINAIS

9.1 Casos excepcionais ou não contemplados pela PCSI devem ser tratados individualmente, mediante orientação da unidade gestora de Segurança da Informação.

9.1.1 Eventualmente, por decisão da unidade gestora de Segurança da Informação ou para resolução de conflitos, o Comitê de Segurança da Informação poderá ser envolvido e chamado a manifestar-se em casos excepcionais.

9.1.2 O Comitê de Contingência, quando instaurado, poderá excepcionalizar temporariamente controles de Segurança da Informação, quando tais controles inviabilizarem a execução dos procedimentos de recuperação necessários.

9.2 A unidade gestora de Segurança da Informação pode propor a implantação de controles adicionais para atingir os objetivos definidos na seção 1, desde que de acordo com os princípios desta PCSI.

9.3 Havendo modificação na nomenclatura ou na competência das Unidades Fundamentais e Unidades Administrativas Principais da estrutura organizacional do Sistema BNDES, ou a atualização de normativos, o presente ato normativo permanecerá em vigor, adequando-se a sua aplicação às novas normas da organização interna.

9.4 O prazo previsto para revisão desta Política é anual, em conformidade com a Resolução CMN nº 4.893 de 2021.

9.4.1 A revisão anual será submetida diretamente à manifestação do Conselho de Administração do BNDES sempre que não houver necessidade de alteração na Política em vigência ou nas situações em que a proposta se enquadrar nas seguintes hipóteses:

a) a alteração tiver como finalidade mera adequação a normativo externo de reprodução obrigatória; e/ou
b) a alteração tiver como finalidade a correção de erro material; e/ou
c) a alteração tiver como finalidade adequar a redação da Política às modificações realizadas na estrutura organizacional do Sistema BNDES, desde que a proposta se limite a alterar siglas/nomes de unidades e/ou sugira a redistribuição dos papéis e responsabilidades já previstos no

normativo, de forma a adaptar a Política ao disposto na Organização Interna Básica do Sistema BNDES em relação às atribuições das Unidades Fundamentais (UF) e/ou das Unidades Administrativas Principais (UAP).

9.4.1.1 Previamente à manifestação do Conselho de Administração, será feito comunicado à Diretoria Executiva, ao Comitê de Riscos e, eventualmente a outro órgão colegiado sempre que exigido por normativo externo.

9.4.1.2 A proposta de revisão não seguirá este trâmite nos casos em que, ao se manifestar sobre a matéria, o Conselho de Administração entenda pela impossibilidade de adoção do fluxo de aprovação simplificada.

9.5 O presente ato normativo entrará em vigor na data de sua publicação no Portal de Normas, revogando-se a Resolução CA nº 20/2023 de 15/12/2023.

Lista de Assinaturas

Assinado por: RAFAEL ESMERALDO LUCCHESI RAMACCIOTTI, 431.***.***-**, assinado em: 24/01/2025
Função: Conselheiro CA / Junta de Administração
Papel: Presidente do Conselho de Administracao do BNDES